

# Notice of Allowability

Application No.

09/275,911

Examiner

Ronald Baum

Applicant(s)

LIU ET AL

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 12/21/2004.
2. ☒ The allowed claim(s) is/are 1,4,5,7,11-14,16,18,19,21,25,26,29,32,34 and 35.
3. ☒ The drawings filed on 24 March 1999 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All b) ☐ Some\* c) ☐ None of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

## Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date 03292005.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

### EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Sharon Wong, Reg. No. 37,760 on 3/30/2005.

1. Replace claims 1,14,26,29,32 and 34 with:

1. A method to bit scramble a digital video signal, comprising:  
receiving blocks of the digital video signal;  
scrambling the blocks of the digital video signal responsive to a key of which  
a remote computer number and  
a video position number are components, the video position number  
representing positional information including the block to be scrambled,  
wherein the scrambling includes XOR operations between  
the blocks of the digital video signal to be scrambled and  
other operands, with each XOR operation being between  
one of the blocks to be scrambled and  
one of the other operands,  
wherein the other operands are each the key.

Art Unit: 2136

14. A method to descramble a bit scrambled video signal in a computer, comprising:  
receiving blocks of the bit scrambled video signal; and  
descrambling the blocks of the bit scrambled video signal responsive to a remote computer number of the computer in which the descrambling is occurring,  
wherein blocks of the digital video signal was scrambled responsive to a key of which  
  
a remote computer number and  
  
a video position number are components, the video position number representing positional information including the block to be scrambled,  
wherein the descrambling includes XOR operations between  
  
the blocks of the digital video signal to be descrambled and  
other operands, with each XOR operation being between  
  
one of the blocks to be descrambled and  
  
one of the other operands,  
  
wherein the other operands are each the key.
26. An article comprising:  
  
a machine readable medium having instructions thereon which when executed by a computer cause the computer to:  
  
receive blocks of the digital video signal; and  
  
scramble the blocks of the digital video signal responsive to a key of which

Art Unit: 2136

a remote computer number and  
a video position number are components, the video position  
number representing positional information including the block to be  
scrambled, wherein the scrambling includes XOR operations between  
the blocks of the digital video signal to be scrambled and  
other operands, with each XOR operation being between  
one of the blocks to be scrambled and  
one of the other operands,  
wherein the other operands are each the key.

29. An article comprising:

a machine readable medium having instructions thereon which when executed by  
a computer cause the computer to:

receiving blocks of a bit scrambled video signal, the blocks of the digital  
video signal scrambled responsive to a key of which

a remote computer number and  
a video position number are components, the video position  
number representing positional information including the block to be  
scrambled, wherein the scrambling includes XOR operations between  
the blocks of the digital video signal to be scrambled and  
other operands, with each XOR operation being between  
one of the blocks to be scrambled and

one of the other operands,

wherein the other operands are each the key; and

descrambling the blocks of the bit scrambled video signal.

32. A computer system comprising:

a scrambling device to

receive blocks of a digital video signal and

scramble the blocks of the digital video signal responsive to a key of

which

a remote computer number and

a video position number are components, the video position  
number representing positional information including the block to be  
scrambled,

wherein the scrambling includes XOR operations between

the blocks of the digital video signal to be scrambled and

other operands, with each XOR operation being between

one of the blocks to be scrambled and

one of the other operands,

wherein the other operands are each the key.

34. A computer system comprising:

a descrambling device to

Art Unit: 2136

receive blocks of a bit scrambled video signal and  
descramble the blocks of the bit scrambled video signal responsive to  
a remote computer number of the computer system in which the  
descrambling is occurring and  
a video position number,  
wherein the descrambling includes XOR operations between  
the blocks of the digital video signal to be descrambled and  
other operands, with each XOR operation being between  
one of the blocks to be descrambled and  
one of the other operands,  
wherein the other operands are each the key.

2. Cancel claims 6 and 20.

***Examiner's Statement of Reasons for Allowance***

3. Claims 1,4,5,7,11-14,16,18,19,21,25,26,29,32,34 and 35 are allowed over prior art.
4. This action is in reply to applicant's correspondence of 21 December 2004
5. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.
6. As per claims 1,14,26,29,32 and 34, prior art of record, Ibaraki et al, U.S. Patent 5,546,461, Chapman, U.S. Patent 6,173,402 B1, Faria, UK Patent Application GB 2316278A, SCHNEIER, BRUCE, Applied cryptography, second edition, John Wiley & Sons, Inc. 1996,

Art Unit: 2136

pages 193, section 9.3, 1<sup>st</sup> paragraph, IDS paper No. 4, and Dent, U.S. Patent 5,091,942, fails to teach, alone, or in combination, of;

(Claim 1)     “A method to *bit scramble a digital video signal*, comprising:  
receiving *blocks* of the digital video signal;  
*scrambling the blocks* of the digital video signal *responsive to a key* of which  
a *remote computer number* and  
a *video position number* are components, the video position number  
*representing positional information including the block to be scrambled*,  
wherein the scrambling includes *XOR operations between*  
*the blocks* of the digital video signal to be scrambled and  
*other operands*, with each XOR operation being between  
one of the blocks to be scrambled and  
one of the other operands,  
*wherein the other operands are each the key.*”

7.     The *italicized* above claim elements dealing with (for example; claim 1) “ ... *bit scramble a digital video signal...blocks ... scrambling the blocks ... responsive to a key ... remote computer number ... video position number ... representing positional information including the block to be scrambled... XOR operations between the blocks ... other operands...wherein the other operands are each the key.*” serving to patently distinguish the invention from prior art. Specifically, while the use of cryptographic and scrambling/ de-scrambling keys generally

Art Unit: 2136

generated via various pseudo-random number generation schemes for the purpose of providing data stream and general content security, is known in the prior art (i.e., see "Cheng, Jieylin, et al, "STREAMTO: Streaming Content Using a Tamper-Resistant Token", Univ. of Twente, 2003, entire document, [www.ub.utwente.nl/webdocs/ctit/1/0000011c.pdf](http://www.ub.utwente.nl/webdocs/ctit/1/0000011c.pdf)), the use of specific key generation involving the use of the digital content block formatted (i.e., stream protocol) "video position number" combined ("the other operand") with the use of a remote or receiving device "computer number", is patently distinct in the art. More specifically, the XOR operation to scramble the digital data blocks with said generated key (i.e., logical KEY XOR DATA on a block to block basis per se) is not taught in the art. Further, the reverse de-scrambling process using the analogous key parameters against the recipient device data stream is likewise not taught in the art (i.e., the claim 14 de-scrambling limitations).

As per the applicants arguments in the previous remarks in the Amendment (of 21 December 2004), the examiner finds the applicant's arguments to be persuasive in that the art of record does not teach or suggest the use of "video position number" combined ("the other operand") with the use of a remote or receiving device "computer number", let alone provide a motivation to combine such elements, so as to therefore patently distinguish the invention from the prior art of record.

However, the claim language clearly associates the applicant's invention to the scrambling of "*digital video [data] signal[s]*" per se (i.e., pay television, or streaming network content), and further that the key consisting of the "*video position number*" combined ("*the other operand*") with the use of a remote or receiving device "*computer number*", clearly must be *logically XOR'd with the data specifically on a block to block basis*, versus the obfuscation of the data via a non-block protocol using key not directly XOR'd with the content data. This is in



Art Unit: 2136

contrast to non-streaming type of non-video content (i.e., digitized music or software content) in passive storage environments and technologies in general (i.e., data stored on a CD, DVD, removable media, etc.).

8. Dependent claims 4-7, 11-13, 16, 18-21, 25 and 35 are allowable by virtue of their dependencies.

Art Unit: 2136

***Conclusion***

9. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 703-872-9306.

Ronald Baum



Patent Examiner

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100